

**Identity Management in Financial Institutions:**

# A Focus on the CIO

---

**Addressing Key Concerns of CIOs:**

- Compatibility With Other IT Systems
- Customization Maintenance
- Regulatory and Compliance Requirements
- Digital Transformation

# A Letter from the Co-Founder and CEO

---



Over the last decade, I have spoken to dozens of Chief Information Officers (CIOs) to understand their Identity Governance and Administration needs and the complexity of their IT leadership roles. This document is designed as a short brief for those executives making critical decisions about their institution's technology infrastructure.

At Evolveum, our first and primary focus is on developing midPoint, striving to make it the world's best identity management and governance platform for complex organizations. We are thrilled that midPoint, as the only open source platform, has been recognized as a complete IGA suite by Gartner and KuppingerCole.

Everything we do is open source, which helps CIOs understand how midPoint works and gives them more control over their infrastructure. We are in continuous dialogue with identity engineers, privacy officers, security experts, open source enthusiasts, system developers, and administrators worldwide who challenge our thinking to make the midPoint IGA platform stronger. We believe sharing is caring.

Dealing with legacy systems, virtual working environments, and changing customer behavior drive the need for increased security, especially in the area of data protection. Solving these data protection problems through automation requires answers for IT security experts and top leaders in IT. Moreover, the financial services industry is one of the most regulated industries, and CIOs must demonstrate strong access controls to auditors and regulators.

I hope you will find answers to your questions and concerns on the following pages. Thank you for considering Evolveum's midPoint product for your organization's identity governance and administration needs.

Best regards,

A stylized, handwritten signature in black ink, appearing to read 'Igor Farinic'.

Igor Farinic

# Addressing Frequent Questions Faced by CIOs

---

We are pleased that many security professionals and identity experts have chosen the midPoint platform. Their subject matter expertise enables them to granularly examine the mechanisms which can deliver strong enterprise identity governance and automation.

Most financial institutions look to build a unified identity layer on top of their existing infrastructure. This enables them to create and manage user information, add new business rules, and then seamlessly synchronize it with services and other repositories, ensuring identity data is always up-to-date.

The process of gaining organizational acceptance of a specific identity management product also requires examining several broader factors. We've listened to CIOs and consistently heard these five questions rise to the top:

---

1

How compatible is midPoint with systems in the financial services environment?

---

2

How can Evolveum help organizations keep customization maintenance to a minimum?

---

3

How can midPoint protect data and help fulfil regulatory and compliance requirements?

---

4

How can midPoint help me accelerate the digital transformation?

---

5

Why should I consider including an open source IGA platform in my infrastructure?

# #1 How compatible is midPoint with systems in the financial services environment?

MidPoint provides countless connectivity possibilities across a broad array of systems.

With midPoint, financial institutions make no compromises, and they are free to choose if they want deployment to be in the cloud, hybrid, or on-premise.

MidPoint supports a wide range of protocols and standards, including LDAP, Kerberos, SAML, OAuth, OpenID Connect, SCIM, and RESTful APIs, making it easy to integrate with various systems and applications. It also offers pre-built connectors for many popular systems and applications, including Microsoft Active Directory, Office 365, Salesforce, SAP, and more.

MidPoint's RBAC (Role-Based Access Control) system allows financial institutions to easily manage access rights and permissions across their entire IT environment. This makes it easy to ensure that users have the right level of access to the systems and applications they need to do their jobs, while also maintaining security and compliance.

The open source nature of midPoint also allows integrators to create new connectors that meet the specific needs of organizations, enabling the seamless integration of midPoint with the systems they use. Evolveum and their official partners continuously work to develop more tools and integrations, expanding midPoint's compatibility with different systems.



## #2 How can Evolveum help organizations keep customization maintenance to a minimum?

Effective identity management lies at the core of any IT infrastructure. When it comes to something as fundamental as IdM, organizations seek to avoid being forced into a rigid, monolithic package that requires them to change their business practices to fit the package's capabilities. Luckily, midPoint provides a flexible and adaptable platform that can be customized to meet an organization's unique needs. It can help financial institutions handle customizations in a seamless way by:

**New Feature Development:** Thanks to Evolveum's subscription model<sup>1</sup>, midPoint customers have the privilege of being able to influence the product roadmap and have new features developed for their use case. These features become part of the midPoint product, so there are no limitations or extra maintenance required for customizations.

**Seamless Upgrades:** Because new features are integrated into the midPoint product, midPoint customers can upgrade without having to worry about additional customization maintenance. Evolveum's team takes care of ensuring that customizations remain compatible with new versions of the platform.

**List of Open Source Connectors:** The midPoint platform includes supportable connectors that can integrate with a wide range of systems, applications, and directories. This reduces the need for custom coding and minimizes the time and effort required to maintain these integrations.

**Configurable Workflows:** MidPoint allows financial institutions to configure workflows and business rules to automate IAM processes. This reduces the need for custom development and makes it easier to modify these processes as business needs change.

**Flexible and Configurable:** MidPoint was designed to be flexible and adjust to organizations' needs, and not vice versa. This means that financial institutions can customize the platform to their specific business needs without having to undergo extensive development work themselves.

---

<sup>1</sup> Applicable to specific subscription models

## #3 How can midPoint protect data and help fulfil regulatory and compliance requirements?

---

The volume of data has been steadily increasing with no sight of slowing down. Nowadays, it is imperative to understand who has access to what at any given time. CIOs need reliable, flexible, and effective tools to be able to protect data, demonstrate strong access controls to auditors, and satisfy regulatory and compliance requirements.

MidPoint is a powerful platform with a range of capabilities to assist CIOs in achieving these colossal tasks. They include:

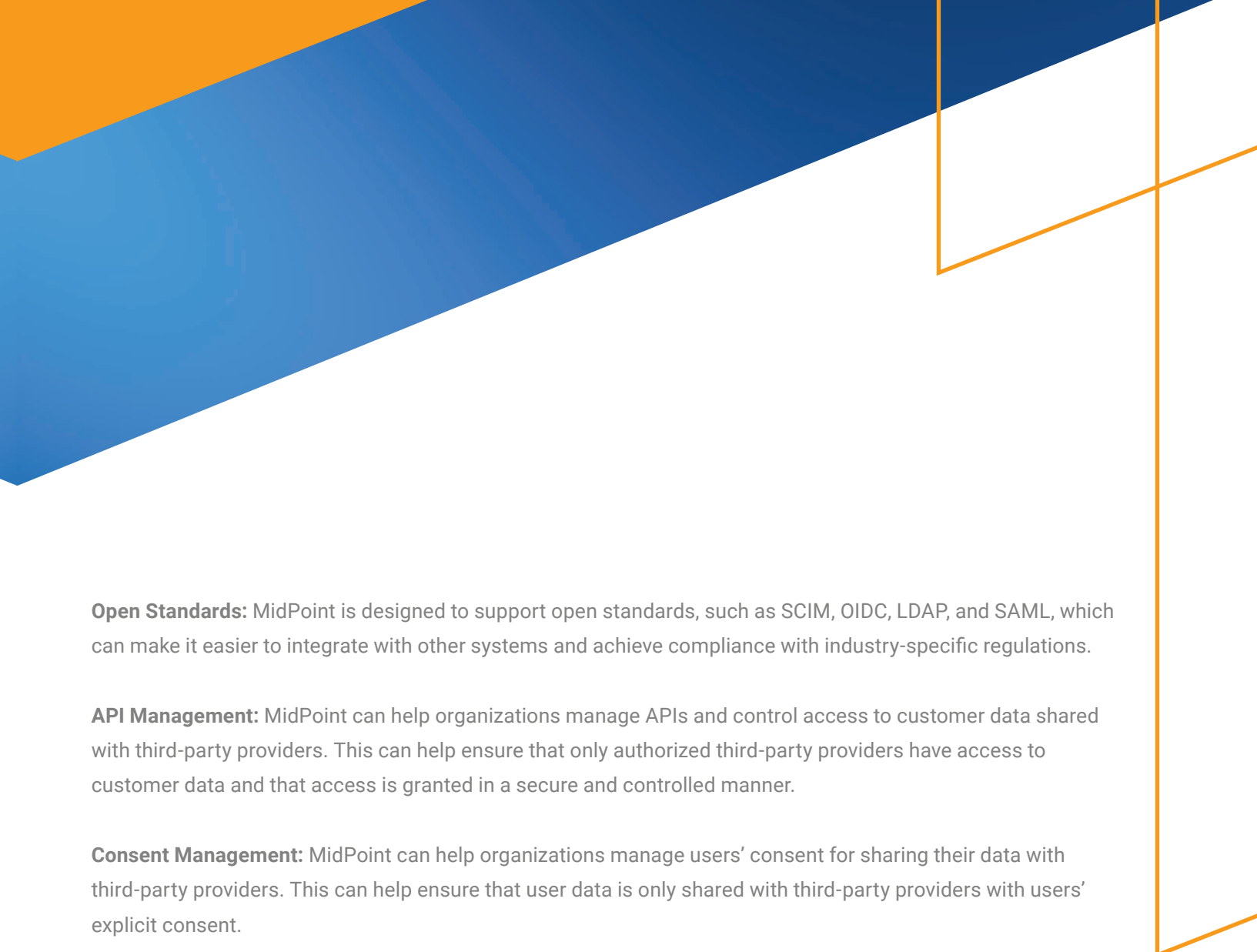
**Access Control:** MidPoint allows access policies to be defined based on roles and responsibilities. This ensures that users only have access to the data they need, reducing the risk of unauthorized access to sensitive information. MidPoint implements role-based access controls, enforces strong password policies, and conducts regular access reviews.

**Provisioning and Deprovisioning:** MidPoint automates the provisioning and deprovisioning of user accounts and access rights, ensuring that access is only granted when needed and revoked when no longer required. This reduces the risk of orphaned accounts and access rights, which can be exploited by attackers to gain unauthorized access.

**Auditing and Reporting:** MidPoint provides detailed auditing and reporting capabilities. This allows user activity and access events to be tracked, potential security threats to be detected, and helps with the generation of compliance reports. It can generate audit trails of all access events, such as authentication attempts, system changes, and data access.

**Identity Governance:** MidPoint manages identities and their associated attributes, such as department, and location, which provide a centralized view of user identities. It can identify and remediate orphaned accounts and enforce separation of duties (SoD) controls.

**Workflow Automation:** MidPoint can automate workflows related to access requests, approvals, and certifications, reducing the time and effort required to manage access.



**Open Standards:** MidPoint is designed to support open standards, such as SCIM, OIDC, LDAP, and SAML, which can make it easier to integrate with other systems and achieve compliance with industry-specific regulations.

**API Management:** MidPoint can help organizations manage APIs and control access to customer data shared with third-party providers. This can help ensure that only authorized third-party providers have access to customer data and that access is granted in a secure and controlled manner.

**Consent Management:** MidPoint can help organizations manage users' consent for sharing their data with third-party providers. This can help ensure that user data is only shared with third-party providers with users' explicit consent.

**Data Deletion:** MidPoint can help organizations delete users' personal information when required. This includes automated workflows for identifying and deleting personal information, as well as audit trails to document the deletion process.

The financial services industry has gone through significant changes in recent years, which have resulted in increased threats in the area of information security. The industry had to adapt to remote work during the pandemic, which led to an increased reliance on cloud services and VPNs. Moreover, attackers have taken advantage of these changes and launched frequent and detrimental cyber-attacks. The financial services industry has also faced security challenges related to mergers and acquisitions, supply chain security with third-party vendors, and increased digitization. While complying with regulations is an important step in protecting systems and data, it is not enough on its own. CIOs need to take a proactive approach to cybersecurity to be able to keep up with rapidly evolving cyber threats.

# #4 How can midPoint help me accelerate the digital transformation?

The financial services industry has experienced significant changes in customer behavior in recent years, driven by several factors such as technological advancements, changing customer preferences, and increased competition. In today's rapidly evolving digital landscape, financial institutions must provide a secure, efficient, convenient, and modern digital experience. MidPoint can help lead the change in the following areas:

## 1. Connecting Legacy Systems

Identity management is at the core of every company's IT infrastructure. Given the prevalence of legacy and homegrown systems, the first step financial institutions need to take to achieve digital transformation is to consolidate these disparate systems into a unified solution. MidPoint is a customizable platform, and thanks to a smart connector mechanism, it enables the connectivity between midPoint and these critical legacy systems.

## 2. Improving Operational Efficiency

MidPoint can help financial institutions streamline processes and reduce the workload on their IT departments by automating user provisioning and deprovisioning, access requests, role management, and access certifications, among other things. This improves operational efficiency and reduces the risk of errors, delays, and security breaches.

## 3. Enhancing User Experience

Users now require a seamless digital experience that they are in control of. MidPoint's self-service capabilities allow users to request access to resources, reset passwords, and update their profiles, reducing the workload on IT departments and improving user experience. In addition, midPoint's user intuitive interface makes it easier for administrators to manage user access and governance policies.

Implementing multi-factor authentication (MFA) is another way to further secure access to sensitive data and systems. MidPoint's MFA capability adds an additional layer of security by requiring users to provide two or more authentication factors to verify their identity.

MidPoint can also support digital business initiatives such as cloud adoption by providing secure access to resources from any location or device.

With increased automation, valuable resources are saved, allowing for further investment in modernizing the entire IT environment.



## #5 Why should I consider including an open source IGA platform in my infrastructure?

Evolveum believes in the full transparency it provides; midPoint has the entire source code completely open without any proprietary parts. This provides financial institutions with a better understanding of how midPoint works and gives them more control over their infrastructure. Moreover, the visibility of each line of the source code brings heightened visibility and full auditability. Everyone can see the code, which makes it more secure, and security issues can be identified and escalated to Evolveum quickly.

Vendor lock-in can be avoided by using an open source software. MidPoint gives its users the freedom to work with a variety of systems and the possibility to change them anytime. A library of connectors with open code speeds up integration efforts and brings skilled teams a valued opportunity to fix the bugs found in the connectors themselves. Additionally, there is the option to leverage support from Evolveum and their official partners.

MidPoint can be used freely without the need to purchase licenses. The budget to maintain and develop midPoint comes from support services.

Evolveum uses a professional open source business model, which means that institutions can rest assured knowing that technical support is available when they need it. By activating a subscription<sup>1</sup>, Evolveum's technical team handles products bugs, product failures, develops missing features, improves product documentation, and provides product samples.

The entire midPoint project is guided by the genuine definition of the open source philosophy. Everything is visible to the public – whether it's the source code, issues reported in the Jira ticketing system, technical documentation, or design documents. Institutions can download and test midPoint without any restrictions or barriers such as having to provide an email address to start. Moreover, they can take advantage of the community's effort and download midPoint in one of the 20 languages it has been translated into. The community also publishes connectors' code, writes tests for bugs and features, and answers questions on the mailing lists, to name a few.

---

<sup>1</sup> The services listed depend on the type of subscription you activate

# References



## **BRANDON POWERS**

*Product Manager and Lead Software Engineer, Provision IAM*

“Protecting customer data is of utmost importance to banks, and they adhere to strict regulations to ensure it. For a long time, they have been implementing the concept of least privilege through defining role-based access control (RBAC) policies. However, enforcing least privilege remains a challenge due to the numerous legacy systems in place.

With midPoint, this challenge becomes much easier as it offers highly customizable IGA solutions that not only record RBAC policies but also govern them through a wide range of connector types, lifecycle policies, certification campaigns, and customized reporting. It’s a proven solution that banks can rely on to enhance their data protection efforts.”



## **MATT GROWDEN**

*CISSP, former CIO and virtual CIO of community bank*

“As a former bank CIO and consultant, I was used to spending effort on manual processes to set, enforce, maintain, and audit access control policies and identity lifecycles for numerous systems. Unfortunately, manual processes do not scale well and leave you open to unnecessary risk.

MidPoint’s ability for customization, especially regarding resource connectors, enables the connectivity of critical legacy systems which are all too common in the financial industry. I was very impressed with midPoint’s ability to be the single source of identity governance and administration and equally impressed by how audits and examinations were handled more completely and easily.”

# References



## **SVEN LUKRAFKA**

*Senior IAM Consultant, DAASI International*

“MidPoint is well equipped to work in the financial service environment as it allows for the implementation of complex requirements, especially with regard to security and auditing processes. Moreover, the wide range of out-of-the-box features in midPoint help to keep the need for customization at a minimum. Additionally, midPoint’s internal interfaces across releases allow for a smooth upgrade and/or enhancement process.

With the creation of guidelines and policies within midPoint, even the more complex requirements of financial service providers can easily be met. In particular, the rich set of features for audits also allows various past states to be precisely reproduced. Lastly, because midPoint is open source, potentially needed extensions are usually fairly easy to access or can be programmed by a preferred partner of Evolveum. If there are any problems, there is a whole community in place to quickly provide a solution.”

# Evolveum

For further information, please contact us at  
[cio@evolveum.com](mailto:cio@evolveum.com)